ANNEX A

Business Enterprise Architecture

System Compliance Assessment

Version History

Version	Publication Date	Author	Description of Change
1.0 Draft	January 31, 2003	Roy Gibbs	Initial Release (Draft)
2.0 Final	March 14, 2003	Roy Gibbs	Updates to reflect Government feedback on 1.0 Draft
3.0 Draft	April 8, 2003	Monica Davis Roy Gibbs Sharon Klugiewicz Grant Soderstrom	Updates to reflect Government discussions, addition of weightings, provision of architecture product reference documentation
3.0 Final	April 25, 2003	Monica Davis Roy Gibbs Sharon Klugiewicz Grant Soderstrom	Updates to reflect Government comments
4.0 Draft	August 1, 2003	Monica Davis Scott Young Aly Zein	Updates version 3.0 and changes document title
4.1 Draft	September 15, 2003	Monica Davis Aly Zein	Updates reflect Government comments.
4.1 Draft	September 27, 2003	Monica Davis Aly Zein	Updates reflect Government comments.
4.2 Draft	October 22, 2003	Patty St. George Monica Davis Aly Zein	Updates reflect Government comments.

Table of Contents

Index of Tables

Index of Figures

Appendices

Acronym List

AOA	Analysis of Alternatives
APB	Acquisition Program Baseline
AV-1	BEA Overview and Summary Information
BEA	Business Enterprise Architecture
BMMP	Business Management Modernization Program
BMSI	Business Modernization and Systems Integration
CAA	Command Architecture Assessment
CCA	Clinger-Cohen Act
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
CDD	Capability Development Document
CPD	Capability Production Document
DoD	Department of Defense
DoDAF	DoD Architecture Framework
EA	Economic Analysis
FMEA	Financial Management Enterprise Architecture
ICD	Initial Capabilities Document
IT	Information Technology
MAIS	Major Automated Information System
OMB	Executive Office of the President, Office of Management and Budget
OV	Operational View
OV-3	Operational Information Exchange Matrix
OV-5	Activity Model
OV-6a	Operational Rules Model
SV	Systems View
SV-1	System Interface Description
SV-4	System Functionality Description
SV-6	System Data Exchange Matrix
TV	Technical View
TV-1	Technical Architecture Profile

References

The following table lists the documents used or referenced in this document.

	Referenced Document
1	Business Management Modernization Program, Program Management Office, *BMMP Compliance Plan*, draft issued June 6, 2003.
2	Business Management Modernization Program, Program Management Office, *BMMP Transition Plan*, Call 0006, draft issued June 6, 2003.
3	Clinger-Cohen Act of 1996 (formerly, Information Technology Management Reform Act [ITMRA]), Public Law 104-106, February 10, 1996.
4	Chief Information Officers Council, *Architecture Alignment and Assessment Guide*, October 2000.
5	Defense Authorization Act of 2003, Public Law 107-314.
6	Defense Authorization Act of 2003, Public Law 107-248 Section 8088
7	Department of Defense Appropriations Act, 2004, Public Law 108-87
8	Department of Defense, Draft Department of Defense Instruction, *DoD Architecture Framework, Volume III, Version 1.0*, October 1, 2001.
9	Business Enterprise Architecture (BEA) Description of Leading Practices Update #1, Version 1.0 (Draft), 25 July 2003
10	Business Management Modernization Program, *FMEA Overview and Summary Information AV-1*, Call 0006 Version 5.0, Draft, July 30, 2003

1. Introduction

The Secretary of Defense established the Business Management Modernization Program (BMMP) to provide policy direction and oversight for business management modernization efforts. While prudent investments in operational, developmental, and new system initiatives are important to maintain and improve the Department's business operations, the overall alignment and compliance with the Department's Business Enterprise Architecture (BEA) must be assessed.

The system assessment process supports the compliance requirements of the Clinger-Cohen Act, Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, and Public Law 107-314, *The Defense Authorization Act of 2003*, which require that regular assessments be conducted of the BEA and its components.

On April 23, 2003, the BMMP issued the *Financial Management Enterprise Architecture (FMEA) Criteria for Assessing Compliance Against the Architecture*, that document provided an initial "system assessment process and evaluation criteria to evaluate BEA system compliance from the business management and system technology perspectives." This document updates that process by providing assessment and evaluation criteria and a step-by-step process for completing a system compliance assessment in relation to the BEA.

This document forms the core system assessment criteria for all Domains to demonstrate compliance with the BEA. In addition, Domains may choose to append additional criteria for the assessed systems.

1.1 Purpose

This document provides a system assessment process that will satisfy BMMP requirements for system compliance and Public Law 107-314 Section 1004 requirements for a ".. determination that the defense financial system improvement is consistent with both the enterprise architecture and transition plan." It also, satisfies Public Law 107-248 Section 8088 "Certifications as to Compliance with Financial Management Modernization Plan" and Public Law 108-87 "Certifications as to Compliance with Financial Management Modernization Plan."

The process and evaluation criteria established here facilitate the system assessment process by providing guidance for assessing systems under development, new acquisition solutions, and operational systems with a current year investment budget of greater than $1,000,000 for BEA compliance. References to the term "system" in this document apply to systems under development, new acquisition solutions, and system change requests unless noted otherwise. This standardized approach will result in a more consistent application of criteria during the assessment process. Reference to the term "system entity" in this document refers to system applications.

Throughout this document, the term 'alignment' means that the system can be properly identified to the relevant parts of the BEA based on the architecture definitions, e.g., for operational activity, system entities/function, and interfaces. A system is aligned if a relationship is established for all architecture elements of the system (operational activity, system function, interfaces, etc.) with the corresponding elements of the BEA architecture. I.e., the scope of the system is known in terms of and consistent with the BEA and there are no gaps.

Throughout this document, the term 'compliance' means that the system fully implements the requirements described or referenced by the architecture, e.g., operational business rules descriptions, referenced technical standards or operational controls (policy), respectively. A system is compliant if it imposes the BEA criterion or the referenced architecture model or document as a constraint on its implementation.

1.2 Scope

The scope of this document is to provide process and methodology for conducting a system self-assessment and evaluating that assessment against the “To Be” architecture of the BEA. The BEA requirements are used as the basis for this system assessment process.

The assessment of the business processes and financial related aspects (e.g., return on investment) of systems are beyond the scope of this document.

The BEA System Compliance Assessment provides the guidelines to assess and evaluate system compliance with the objectives of the BEA at the enterprise, technical, operational and systems levels. Applicable systems to be assessed by this process are systems under development, new acquisitions, and operational systems with a current year investment budget of greater than $1 million.

Tools may be applied to automate the processes presented in this document; however, tool selection is beyond the scope of this document.

1.3 Requirements of the Performance Work Statement

The contractor shall recommend criteria to assess compliance with the BEA based on architecture-derived requirements, and submit to BMMP for approval.

1.4 Deliverable Description

This document describes the system compliance assessment and evaluation process, which consists of the context criteria, functional criteria, and technical criteria processes, as well as the system assessment rating for compliance with the architecture.

1.5 Criteria for Acceptance

The deliverable will provide updated criteria for assessing a system’s compliance with the BEA requirements and objectives.

1.6 Document Organization

This document is comprised of five (5) sections outlining the assessment process and eight (8) appendices comprised of reference materials and checklists that facilitate the self-assessment and evaluation processes. See the Table of Contents for a detailed breakdown of the document's outline.

2. Key Concepts

Key concepts are critical in the understanding and development of a System Compliance Assessment process. The key concepts that follow are listed in the order that they appear in the document.

2.1 Context for System Assessment

While this document provides a system compliance assessment process that will satisfy BMMP requirements for system compliance with the BEA, Public Law 107-314 Section 1004, Public Law 107-248 Section 8088, and Public Law 108-87 indicates it must do so in a way that integrates with existing and planned DoD processes. As a result, the system compliance assessment process established here will be an integral part of the Acquisition Framework.

2.2 System Compliance Assessment

The System Self-Assessment consists of three categories of criteria: Context, Functional, and Technical. These categories must be assessed sequentially. Systems must receive an adequate rating for Context criteria prior to assessing the Functional criteria, and receive an adequate rating for Functional criteria prior to assessing the Technical criteria. The sequenced approach for the system compliance assessment allows the process to be terminated early on if a system is deemed non-compliant with either Context or Functional Criteria. The System Program Manager will self assess a rating of red, yellow, or green for each category (refer to Section 5.1 for rating definitions). Only a rating of green or a rating of yellow with a formal documented mitigation strategy will provide the “go-ahead” for the System Program Manager to move forward to the next category of assessment criteria.

After completing the individual assessment for each of the BEA Context, Functional and Technical Assessment Criteria, the System Program Manager will identify the system’s overall compliance with the BEA.

2.3 Evaluation

Lead Domains will coordinate with the partner Domains to evaluate the self-assessment. The "partner" Domains will assess the BEA requirements and objectives within their Domain that pertains to the assessed system. The Lead Domain will perform the overall assessment based on their results and feedback from the partner Domains. The self-assessment is evaluated by reviewing documentation against the self-assessment criteria checklists and determining if compliance is demonstrated accurately with the architecture. The self-assessment is evaluated for its compliance with the Context, Functional, and Technical criteria of the “To Be” architecture. Business Management System Integration (BMSI) will assist with the evaluations until Domains are familiar with BEA.

3. Acquisition Framework

The Defense Acquisition System (DAS) defines the management process by which the DoD provides effective, affordable, and timely systems to the users.

An Acquisition Program is defined as a directed, funded effort that provides a new, improved, or continuing material, weapon system, information system or service capability in response to an approved need.

Defense Business Systems are managed in accordance with DoDD 5000.1 and DoDI 5000.2 unless the Department directs otherwise. Figure 3-1 illustrates the Defense Acquisition framework.

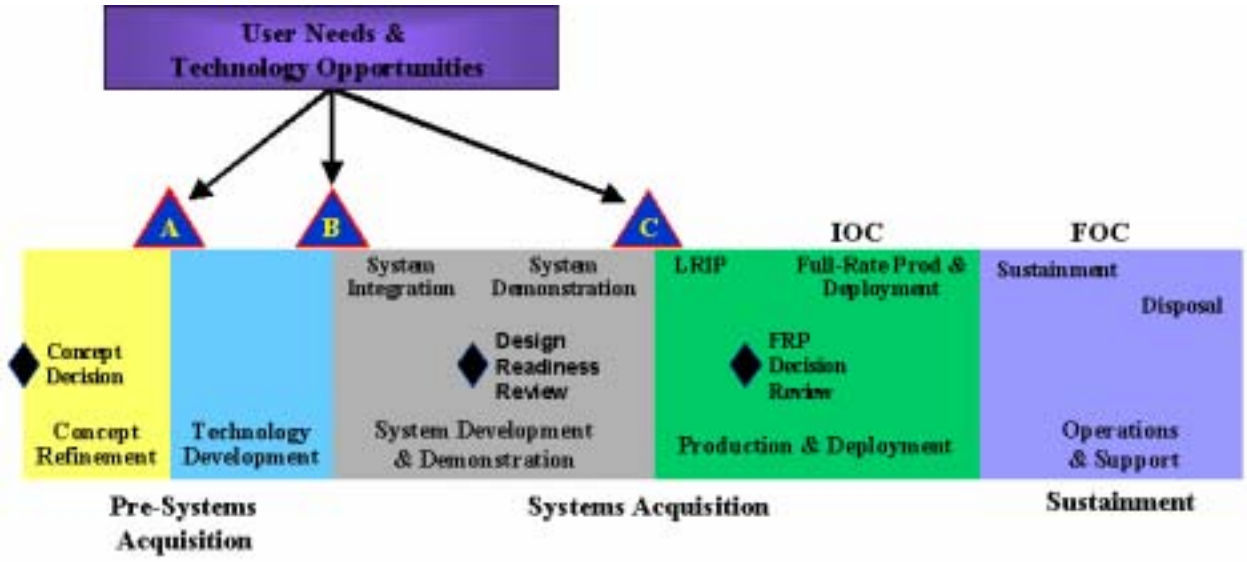

Figure 3-1 Defense Acquisition Framework

The Defense Acquisition Management Framework requires certain statutory and regulatory documentation at pre-designated acquisition milestones. The system compliance assessment process is aligned with the Defense Acquisition Management Framework and allows System Program Managers to capture and include information required by the assessment process within the required Defense Acquisition Management Framework documents or draft documents that are already prepared milestones.

Table 3-1 **gives examples of architectural products that may be used to demonstrate compliance for the self-assessment at each respective acquisition milestone.** This is **not** intended to be a complete list of required documentation. Equivalent documentation is acceptable to demonstrate BEA compliance.

Table 3-1 Work Product Documentation by Milestone

Milestone A	AV-1	SV-1	SV-4	SV-6	OV-3	OV-5	OV-6a	TV-1
Initial Capabilities Document (ICD)	X	X	X	X	X	X	X	X
Capability Development Document (CDD)								
Capability Production Document (CPD)								
Command, Control, Communication, Computers and Intelligence Support Plan (C4ISP)								

Milestone B	AV-1	SV-1	SV-4	SV-6	OV-3	OV-5	OV-6a	TV-1
Initial Capabilities Document (ICD)								
Capability Development Document (CDD)	X	X		X	X	X		
Capability Production Document (CPD)								
C4ISP		X	X	X	X		X	X

Milestone C	AV-1	SV-1	SV-4	SV-6	OV-3	OV-5	OV-6a	TV-1
Initial Capabilities Document (ICD)								
Capability Development Document (CDD)		X		X	X	X		
Capability Production Document (CPD)	X	X		X	X	X	X	X
C4ISP		X	X	X	X		X	X

4. System Assessment Approach

Business management information technology systems are required to be compliant with the BEA. Initially, the Program Manager(s) will conduct a system self-assessment to determine compliance with BEA. These self-assessments consist of a high-level series of specific compliance statements related to BEA compliance requirements at the enterprise, technical, operational, and systems level. These statements, or "criteria", are written to demonstrate and document, where appropriate, a system's compliance with, or mitigation strategy to become compliant with the BEA. Detailing each criterion is a series of questions in the form of a checklist of relevant BEA requirements. A rating of red, yellow, or green is given based on compliance with the criteria.

The following chart is a high level depiction of the self-assessment workflow. The System Criteria Selection consists of providing system information, identifying applicable operational activities and system entities, and transition plan information questions. The initial criteria selection reduces the number of criteria to comply against. The subsequent System Assessment contains workflow seven steps for completing the self-assessment.

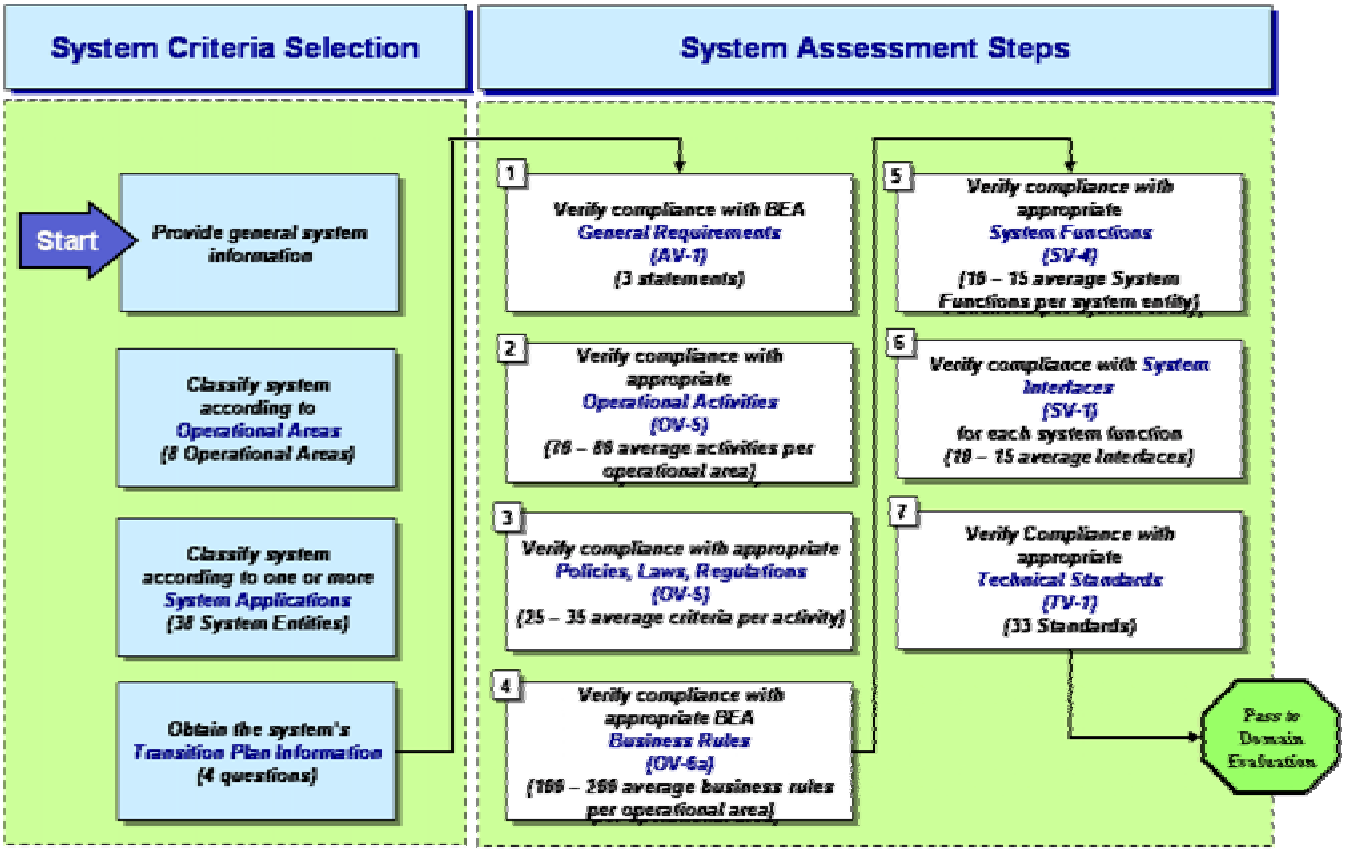

Figure 4-1 System Self-Assessment Workflow

Once the self-assessment is completed, the System Program Manager(s) forwards the completed assessment forms along with the supporting documentation and any mitigation for non-compliant

issues to the Lead Domain for evaluation. The Domain and partner Domains will evaluate the system assessment results to determine the overall level of compliancy with the BEA.

Upon completion of the evaluation of the assessment documentation, the Domain assigns an overall rating of red, yellow, or green to the overall evaluation score. The bulleted list below summarizes the evaluation ratings detailed in Section 5.2.

- A system deemed to be *fully compliant* with the "To Be" architecture is rated as green.
- A system deemed to be *non-compliant* with the architecture is identified by a red rating. To receive a red rating, the system failed to demonstrate mitigation to areas of non-compliance. The system may be re-evaluated if a compliance change is made or mitigation is offered.
- A system deemed to be *substantively compliant* receives a rating of yellow. Yellow signifies that all areas of non-compliance are included in an accepted mitigation strategy that demonstrates the System Program Manager's efforts and plans to achieve compliance in the near future. In those areas in which the system is deemed substantively compliant, the System Program Manager may be requested to address certain compliance issues before proceeding to full implementation.
- A system deemed to be *non-compliant pending architecture change* would receive a rating of red until and unless an architecture change request is approved to address the area of unmitigated non-compliance. The system may be re-evaluated if the architecture change request is approved (or if a compliance change is made or mitigation is offered).

4.1 Assessed Systems

Any defense business system that is currently under development, a new acquisition, and operational systems with a current year investment budget of greater than $1,000,000 must be consistent with the BEA.

4.2 Assessment Criteria

Assessment criteria are high-level BEA compliance statements. A checklist of questions supports the assessment criteria which are contained in Appendices C, D, E, F, G, and H. In completing the self-assessment, the System Program Manager can answer "Yes", "No", or "N/A" (not applicable) to the checklist questions related to their system and provides work products or documentation to demonstrate compliance with the BEA. The System Program Manager will use the BEA System Assessment form, Appendix A, to complete the self-assessment. This form provides step by step instructions to perform the self-assessment.

4.3 Assessment Categories

Criteria for conducting assessments are organized into three categories to aid in the assessment and evaluation process:

1. Context Criteria. Demonstrates a system's compliance with the BEA General Requirements, and alignment with the System Evolution Description (SV-8) within the *BMMP Transition Plan*.
2. Functional Criteria. Demonstrates a system's compliance with the BEA operational activities, operational controls, business rules, system functions, and system interfaces.
3. Technical Criteria. Demonstrates a system's compliance with the BEA Technical Architecture Profile (TV-1).

4.4 Assessment Ratings

Upon completion of the assessment criteria, the Domain Evaluator assigns a rating of Green, Yellow, or Red to each of the three assessment categories, as well as an overall evaluation rating. The assignment of the ratings is explained in greater detail within the context of Assessments (Section 5.1) and Evaluations (Section 5.2).

5. System Assessment and Evaluation Process

The System Compliance Assessment process consists of two steps shown in Figure 5-1 and Figure 5-2. Step A is a self-assessment of the system conducted by the system's Program Manager. Each System Program Manager is responsible for conducting a self-assessment of their system against the BEA criteria. Step B is an evaluation of the program self-assessment conducted by the Domain.

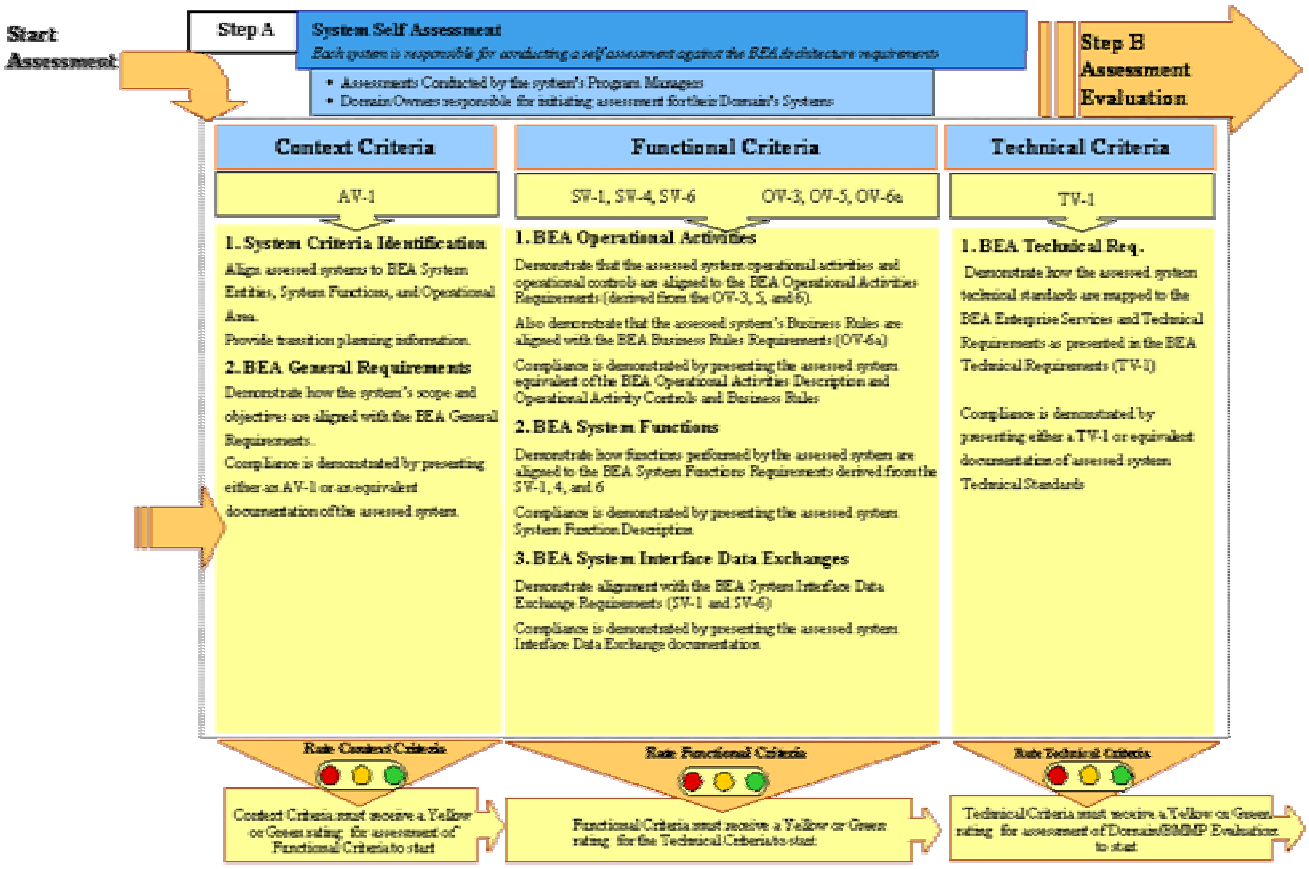

Figure 5-1 Assessment Process Step A

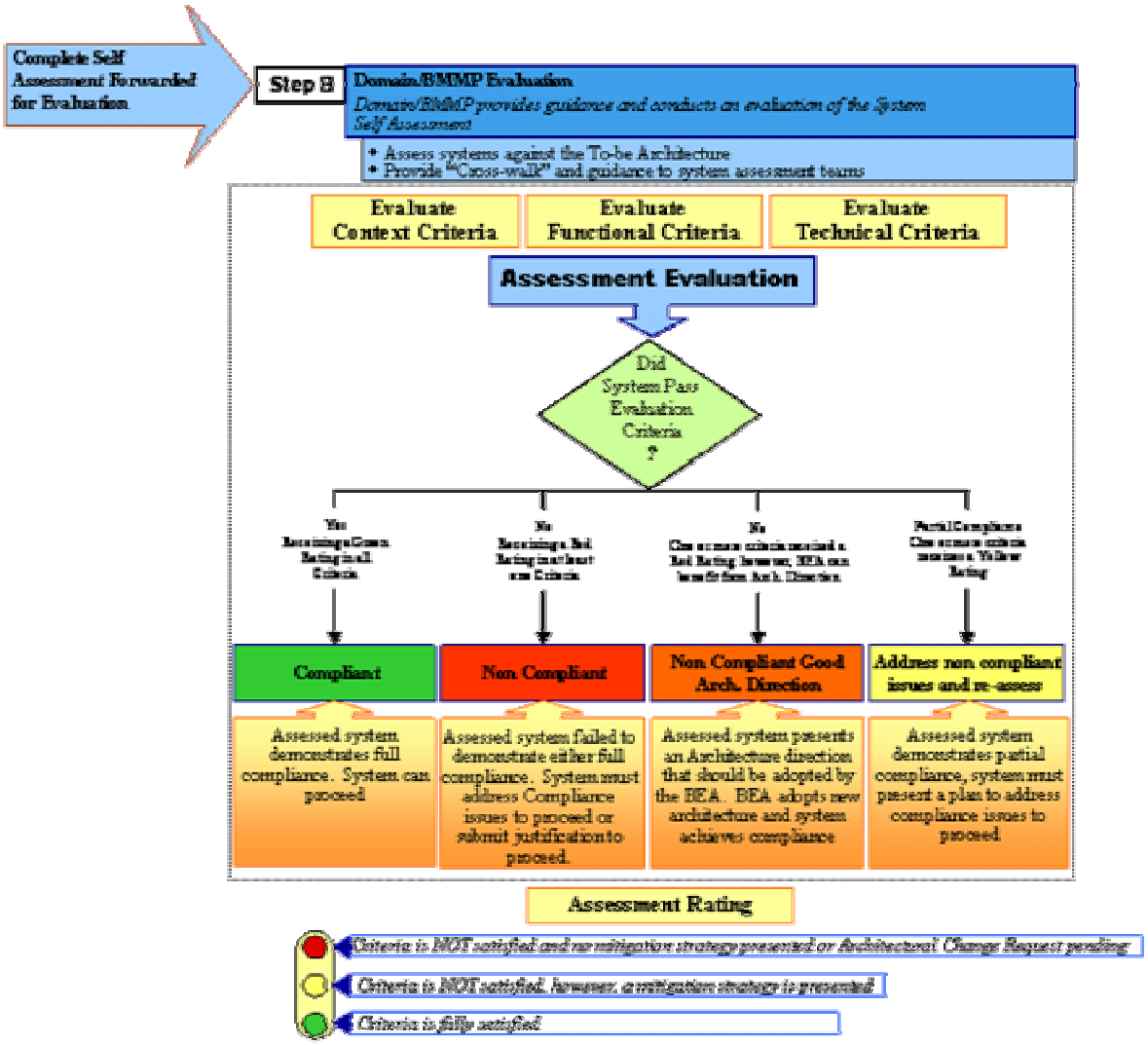

Figure 5-2 Assessment Process Step B

5.1 System Self-Assessment

The System Self-Assessment consists of three categories of criteria: Context, Functional and Technical. The categories must be assessed sequentially. Systems must receive an adequate rating for Context criteria prior to assessing the Functional criteria, and receive an adequate rating prior to assessing the Technical criteria. Within each category, the System Program Manager will self assess a rating of red, yellow, or green, based on the following guidelines:

- A green rating denotes that the system has fully satisfied the required criteria.
- A yellow rating denotes that, while the system may not currently meet the minimum requirements necessary to comply with the BEA, the System Program Manager is providing a mitigation strategy that defines a plan to achieve compliance in the near future.

- A red rating denotes that the system does not meet the minimum criteria required to comply or satisfy the requirements of the BEA, and the system failed to demonstrate mitigation for areas of non-compliance.

The System Program Manager may submit an architecture change request to the Domain (refer to Appendix I) for unmitigated non-compliance. If supported, the Domain will enter the change request into the Project Version Control System (PVCS) Tracker tool for submission to the Configuration Control Board (CCB). The system is re-evaluated if the architecture change request is approved.

Only a rating of green or a rating of yellow with a documented mitigation strategy will provide the "go-ahead" for the System Program Manager to move onto the next category of assessment criteria. If a red rating is received, the System Program Manager may coordinate with the Domain to pursue compliance by providing supporting documentation.

The BEA Systems Assessment form, Appendix A, will be used to record program general information and provide step by step instructions to conduct the self-assessment. After completing the individual assessment for each of the BEA Context, Functional and Technical Assessment Criteria, the System Program Manager will identify the system's overall compliance with the relevant BEA Assessment Criteria by checking one of the following compliance ratings located in Appendix A:

1. ***System is Fully Compliant**: System is compliant with the applicable BEA Criteria*	☐
2. ***System is Partially Compliant**: System is not compliant with one or more BEA Criteria, however, a mitigation is presented*	☐
3. ***System is Conditionally Non Compliant**: System is not compliant with one or more BEA Criteria, however, the System Program Manager recommends submitting a Change Request to BMSI*	☐
4. ***System is Non Compliant**: System is not compliant with one or more BEA Criteria, and a mitigation is not yet defined*	☐

The System Program Manager will deliver the completed assessment to the Lead Domain for evaluation. The Domain will evaluate the three criteria categories of the assessment for its compliance with the of the "To Be" architecture.

5.1.1 Context Criteria

The Context Criteria category consists of two areas:

- BEA Criteria Identification
- BEA General Requirements.

5.1.1.1 BEA Criteria Identification

The first step in the self-assessment process is to establish the assessed system's alignment to the following architecture objects and provide transition planning information.

- BEA System Entities – application system that is comprised of logical groupings of system functions that represent "To Be" system capabilities and requirements.
- BEA System Functions - component applications that performs a specific function.
- BEA Operational Areas - identifies the associated functional process areas of the BEA for a given requirement.

The System Entity(ies) and Operational Areas are the primary architectural objects that enable the self-assessor to establish the scope of the assessment criteria for their system. The BEA System Entity and System Functions will be used to filter and identify the relevant System Functions, System Interface Data Exchanges criteria for assessment. The BEA Operational Areas will be used to filter the BEA Operational Activities and Business Rules for assessment. The operational areas are:

- **ACC –** Accounting
- **CAR –** Collections, Accounts Receivable, and Cash Management
- **FMR –** Financial and Management Reporting
- **HRM –** Human Resource Management (also Medical Heath System Requirements and Travel)
- **LOG –** Logistics
- **PAD –** Procurement, Payables, Acquisition, and Disbursement
- **RPM –** Real Property Management
- **SPB –** Strategic Planning and Budgeting

The following instructions are provided to identify system entity(ies) and system functions related to the assessed system.

1. Go to the "To-Be System Entity 2 To-Be Functions" tab and map the assessed system to BEA System Entity(ies). Select the BEA System Entity(ies) that represents the assessed system by reading the descriptions and determine applicability and alignment. Record the System Entity(ies) in Appendix A, under the General Program Information section. The System Entity will be used as the filter for System Function, System Data Exchanges criteria later in the assessment process.

2. As a result of selecting the relevant entity(ies), column C "System Function" will now list all system functions that correspond to the To-Be System Entity(ies) selected. This list of System Functions will be used throughout the assessment to identify criteria that are applicable to the assessed system**.** Record the System Functions in Appendix A, under the General Program Information section.

3. Go to the "Operational Areas" tab and map the assessed system to BEA Operational Area. Select the BEA Operational Area that represents the assessed system by reading the descriptions applicability and alignment. Record the operational area(s) in Appendix A, under the General Program Information section. The operational area will be used as the filter for BEA Operational Activity, and BEA Business Rules criteria later in the assessment process.

The System Program Manager is also required to provide transition planning information about the assessed system. Table 5-1 contains the four required transition planning questions. The questions are to be answered in Appendix A.

Table 5-1 Transition Plan Questions

Question	
1.	*Is the assessed system replacing an existing system(s)?*
2.	*Identify the system(s) you are replacing.* Provide system name, acronym, POC Name, POC phone number, etc.
3.	*Provide sunset date for the replaced system(s).*
4.	*Provide a detailed transition plan for the assessment system and the replaced system(s) which includes cost and schedule for each system using Microsoft project.*

5.1.1.2 BEA General Requirements

The criteria to assess compliance with the BEA General Requirements consist of questions based on the guiding principles and objectives of the AV-1, Overview and Summary Information. The System Program Manager demonstrates compliance with the BEA general requirements through production of either an AV-1, or an equivalent that satisfactorily supports the assessed response.

The assessed system is required to demonstrate alignment with the BEA General Requirements as outlined in the *FMEA Overview and Summary Information AV-1*[1]. The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA General Requirements:

1. Review the BEA General Requirements document, Appendix C, derived from the BEA AV-1.
2. For each BEA General Requirement listed in Appendix C, thoroughly examine the requirement's definition and determine if the requirement is applicable to the assessed system. For non-applicable requirements, select "N/A" from the drop-down list and provide a detailed and thorough explanation/reason since most general requirements will be applicable.

[1] Business Management Modernization Program, *FMEA Overview and Summary Information AV-1*, Call 0006 Version 5.0, Draft, July 30, 2003.

3. For BEA General Requirements that are applicable to the assessed system, where the system is compliant with the requirement, select "Yes" from the drop-down list and demonstrate the system's compliance by presenting either an AV-1 or equivalent supporting documentation. Provide specific reference to the location within the provided documentation where compliance is specifically demonstrated. This should be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may not be consistent with the evaluator. Clear documentation must be provided to enable the evaluator to quickly and easily locate the specific language/graphics demonstrating compliance and quickly enable a third party audit of any answer.
4. For BEA General Requirements that are applicable to the assessed system, and the system is not compliant, select "No" from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance. Any no answer will constitute a non compliant system.

5.1.2 Functional Criteria

Assessment of the system's Functional Criteria consists of an assessment of specific Systems View (SV) and Operational View (OV) products, as well as relevant external requirements in the following areas:

- BEA Operational Activities - Describes the applicable activities associated with the architecture, the data and/or information exchanged between activities, and the data and/or information exchanged with other activities that are outside the scope of the model (i.e., external exchanges).
- BEA Operational Controls – Controls specify the conditions required for the function to produce correct outputs. Most controls listed in the assessment represent laws and regulations governing those activities/functions in the BEA.
- BEA Business Rules - Describes what the business must do, or what it cannot do.
- BEA System Functions – Component application that performs a specific function
- BEA System Interface Data - Depicts interfaces between system nodes and system entities in terms of required data exchanges that support business activities in the OV.

5.1.2.1 BEA Operational Activities, Operational Controls, and Business Rules

Self-assessment of a system against the BEA operational activities demonstrates that the system's functional activities are mapped to the BEA operational activities requirements (OV-5) and that the assessed system's business rules are aligned with the BEA business rules. The System Program Manager demonstrates operational compliance by presenting the assessed system equivalent of the BEA Operational Activities Description and Business Rules. A checklist is provided in Appendix D to assist the System Program Manager in demonstrating compliance with the BEA operational activities.

The system is required to demonstrate alignment with the BEA Operational Activities Requirements derived from the OV-5, and the BEA Business Rules Requirements derived from the OV-6a. The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA Operational Activities Requirements:

1. Using the selected operational area(s) recorded in Appendix A, filter the BEA Operational Activities Requirements listed in Appendix D.
2. Column B filter should be set to "Activity"
3. Columns C, D, and E list the top level operational activities available for the selected operational area(s).
4. A system will generally support more than one of these operational activities. Read each top level activities supported by your system. This top level activity selection will produce all the leaf level operational activities associated with the top level activity(ies).
5. Column G "Operational Activity" lists all activities that your system must comply with. For each Operational Activity, repeat the following steps to demonstrate compliance:
    a. Review each Operational Activity(ies) in column G.
    b. Thoroughly examine the Operational Activity Description and determine if your system complies with the requirement. For non-applicable requirements, select N/A from the drop-down list in column J and provide detailed explanation, in the Supporting Documentation/Mitigation/Reasoning column, why this activity does not apply to the assessed system.
    c. For BEA Operational Activities Requirements that are applicable to the assessed system and the system is compliant with the requirement, please select Yes from the drop-down list in column J and demonstrate the system's compliance by presenting either an OV-5 or equivalent supporting documentation. Use column K "Supporting Documentation/Mitigation/Reasoning" to provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the page number, paragraph, section number, etc. of the attached documentation. Clear documentation must be provided to enable the evaluator to locate the specific language/graphics demonstrating compliance.
    d. For BEA Operational Activities Requirements that are applicable to the assessed system and the system is not compliant with the requirement, please select No from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance.
    e. The System Program Manager must next assess compliance with each external control that constrains each selected Operational Activity as defined in the BEA. Select "Control" from the drop-down list in column B "Activities/Controls".
    f. Column I "Operational Activities External Controls" lists all external controls that constrain the selected operational activity.

The definition of each control is defined in the "Controls Description" tab in Appendix D.

g. For each Operational Activity External Control, obtain and read the applicable source document and determine whether if your system is in compliance. For non-applicable controls, select N/A from the drop-down list in column J and provide detailed and thorough explanation in the Supporting Documentation/Mitigation/ Reasoning column. It is usually the controls listed on a selected operational activity will be non-applicable.

6. For Operational Activities' External Controls that are applicable to the assessed system and the system is compliant with the control, select Yes from the drop-down list in column J and demonstrate the system's compliance by presenting supporting documentation. Systems at Milestone A should provide documentation that supports compliance or provide a compliance plan for applicable controls. Systems at Milestone B or above should provide documentation that demonstrates compliance. Use column K "Supporting Documentation/ Mitigation/Reasoning" to provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Clear documentation must be provided to enable the evaluator to locate the specific language/graphics demonstrating compliance.
7. For Operational Activities External Controls that are applicable to the assessed system and the system is not compliant, please select No from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance.
8. After assessing all External Controls, change the selection of column B drop-down to be "Activity". Select the next activity from the drop-down list in column G and repeat steps (a) through (j) for all applicable activities.

The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA Business Rules Requirements. Review the BEA Business Rules Requirements document, Appendix E, derived from the BEA OV-6a.

1. Using the operational area selected in Appendix A, filter the BEA Business Rule Requirement listed in Appendix E, Thoroughly examine the Business Rule Description and determine applicability to your system.
2. For BEA Business Rule Requirements that are applicable to the assessed system, where the system is compliant with the requirement, select "Yes" from the drop-down list and demonstrate the system's compliance by presenting either an OV-6a or equivalent supporting documentation. Systems at Milestone A should provide documentation that supports compliance or provide a compliance plan for applicable business rules. Systems at Milestone B or above should provide documentation that demonstrates compliance.

Provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Clear documentation must be provided to enable the evaluator to locate the specific language/graphics demonstrating compliance.

3. For BEA Business Rule Requirements that are applicable to the assessed system, and the system is not compliant with, select "No" from the drop-down list and provide detailed and thoroughly written explanation/reason for non-compliance. For non-applicable business rules, select "N/A" from the drop-down list and provide a detailed and thorough explanation/reason.

5.1.2.2 BEA System Functions

Self-assessment of the system functions demonstrates how they are mapped to the standard BEA system functions as defined in the BEA System Function Requirements. The checklist in Appendix F is provided to assist the System Program Manager in demonstrating compliance with the BEA system functions.

The system is required to demonstrate alignment with the BEA System Function Requirements as outlined in Appendix F. The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA System Function Requirements:

1. Review the BEA System Function document and other Architecture Work Products referenced in Appendix F.
2. Using the selected entities recorded in Appendix A, filter on these Select Entities for the system to obtain the related BEA System Functions in Appendix F. Thoroughly examine each System Function definition and determine applicability. For non-applicable requirements within the filtered list, select "N/A" from the drop-down list and provide a detailed and thorough explanation/reason.
3. For BEA System Functions that are applicable to the assessed system and the system is compliant with the system function definition, select "Yes" from the drop-down list and demonstrate the system's compliance by presenting equivalent supporting documentation. Use the Mitigation/Reason column to provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Clear documentation must be provided to enable the evaluator to easily locate the specific language/graphics demonstrating compliance.
4. For BEA System Function Requirements that are applicable to the assessed system, and the system is not compliant, select "No" from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance. A no response indicates the system is non compliant.

5.1.2.3 BEA System Interface Data Exchange

The third functional criterion that must be assessed is the system's alignment with the BEA System Interface Data Exchange Requirements. The System Program Manager shall demonstrate the system's compliance by presenting satisfactory interface data exchange documentation. The SV-6 in Appendix G is provided to assist the System Program Manager in demonstrating compliance with the BEA system interface data requirements.

The system is required to demonstrate alignment with the BEA System Interface Data Exchange Requirements as outlined in the BEA SV-1 and SV-6. The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA System Interface Data Requirements:

1. Review the BEA System Interface Data Exchange Requirement document, Appendix G.
2. Out-Bound System Data Exchanges:
    a. Using the selected system entity recorded in Appendix A, filter the Sending System Entity "Column A". Column C "Sending System Function" will lists all System Functions within your system entity that communicates with external systems.
    b. Column B and Column D will list the receiving System Entities and System Functions, respectively that the assessed system communicates with.
    c. Column E will list System Data Exchanges (SDEs) that your system shares with the Receiving System Entities and System Functions.
    d. For each SDE, thoroughly examine their description and decide if it is applicable to the assessed system. For non-applicable SDEs, select N/A from the drop-down list of Column G "Compliance" and provide a detailed and thorough explanation/reason.
    e. For SDEs that are applicable to the assessed system, where the system is compliant with the SDE Description, please select "Yes" from the drop-down list and demonstrate the system's compliance by presenting either an SV-1 and SV-6 or an equivalent supporting documentation. Use column H "Mitigation/Reasoning" to provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Identify the interfacing system. Clear documentation must be provided to enable the evaluator to quickly and easily locate the specific language/graphics demonstrating compliance

f. For SDEs that are applicable to the assessed system, and the system is not compliant, please select "No" from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance.

3. In-Bound System Data Exchanges:
   a. Using the selected system entity recorded in Appendix A, filter the Receiving System Entity "Column B". Column D "Receiving System Function" will list all System Functions within your system entity that communicates with external systems.
   b. Column A and Column C will a list Sending System Entities and System Functions, respectively, that the assessed system communicates with.
   c. Column E will list System Data Exchanges (SDEs) that your system shares with the Sending System Entities and System Functions.
   d. For each SDE, thoroughly examine their description and decide if it is applicable to the assessed system. For non-applicable SDEs within the filtered list, select N/A from the drop-down list of Column G "Compliance" and provide a detailed and thorough explanation/reason..
   e. For SDEs that are applicable to the assessed system, where the system is compliant with the SDE Description, please select "Yes" from the drop-down list and demonstrate the system's compliance by presenting either an SV-1 and SV-6 or equivalent supporting documentation. Use column H "Mitigation/Reasoning" to provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Identify the interfacing system. Clear documentation must be provided to enable the evaluator to quickly and easily locate the specific language/graphics demonstrating compliance
   f. For SDEs that are applicable to the assessed system, and the system is not compliant, please select "No" from the drop-down list and provide detailed and thoroughly written explanation/reason for non-compliance.

5.1.3 Technical Criteria

An assessment of the system's technical criteria demonstrates how the assessed system's technical standards (Appendix H) are mapped to the BEA enterprise services and technical

requirements, as presented in the TV-1 (BEA Technical Requirements). The System Program Manager demonstrates compliance with the technical criteria by presenting either a TV-1 or equivalent documentation of assessed system technical standards.

The assessed system is required to demonstrate alignment with the BEA Technical Requirements as derived from the BEA TV-1. The following instructions are provided to assist the System Program Manager in assessing compliance with the BEA Technical Requirements:

1. Review the BEA Technical Standards that applies to the assessed system, thoroughly examine the standard's definition as outlined in the BEA TV-1 and decide if the standard is applicable to the assessed system. For non-applicable standards within filtered list, select "N/A" from the drop-down list in Appendix H and provide a detailed and thorough explanation/reason.
2. For BEA Technical Standards that are applicable to the assessed system and the system is compliant with the standard, select "Yes" from the drop-down list and demonstrate the system's compliance by presenting either a TV-1 or equivalent supporting documentation. Provide specific cite reference to the location within the provided documentation where compliance is specifically demonstrated in the Mitigation/Reasoning block. This could be the section number, paragraph, title, etc. of the attached documentation. The page number should not be used due to reformatting of the document which may be inconsistent with the evaluator. Clear documentation must be provided to enable the evaluator locate the specific language/graphics demonstrating compliance
3. For BEA Technical Standards that are applicable to the assessed system and the system is not compliant, select "No" from the drop-down list and provide a detailed and thorough explanation/reason for non-compliance. Any no answer will constitute a non compliant system.

5.2 Domain Evaluation

5.2.1 Domain Process

The second step in the System Assessment process is a Domain evaluation of the program self-assessment. The System Program Manager will forward the self-assessment to the Lead Domain. In the evaluation process, the Domain(s) will evaluate the self-assessment prepared by the System Program Manager against BEA.

As applicable, lead Domains will coordinate with the other Domains to evaluate the self-assessment. The "partner" Domains will assess the BEA requirements and objectives within their area. The Lead Domain will perform the overall assessment based on their results and feedback from the partner Domains. The self-assessment is evaluated by reviewing the documentation against the self-assessment criteria checklists, validating the "Yes", "No", and "Non Applicable" responses, determining if compliance is demonstrated accurately with the architecture, and acceptance of any mitigating strategies. The self-assessment is evaluated for its compliance with the Context, Functional, and Technical criteria of the "To Be" architecture. It is recommended to have the System Program Manager facilitate a walk-thru with the Lead Domain

to explain the self-assessment results, which will increase understanding and may speed up evaluation process. BMSI will assist with the evaluations until Domains are familiar with BEA.

5.2.2 Evaluation Scoring Process

As with the self-assessment, the Domain assigns an overall rating of red, yellow, or green to the overall evaluation score.

- A system deemed to be *fully compliant* with the "To Be" architecture is rated as green.
- A system deemed to be *non-compliant* with the architecture is identified by a red rating. To receive a red rating, the system failed to demonstrate mitigation to areas of non-compliance. The system may be re-evaluated if a compliance change is made or mitigation is offered.
- A system deemed to be *substantively compliant* receives a rating of yellow. Yellow signifies that all areas of non-compliance are included in an accepted mitigation strategy that demonstrates the System Program Manager's efforts and plans to achieve compliance in the near future. In those areas in which the system is deemed substantively compliant, the system's System Program Manager may be requested to addresses certain compliance issues before proceeding to full implementation.
- A system deemed to be *non-compliant pending architecture change* would receive a rating of red until and unless an architecture change request is approved to address the area of unmitigated non-compliance. The system may be re-evaluated if the architecture change request is approved (or if a compliance change is made or mitigation is offered).

5.2.3 Undersecretary of Defense (Comptroller) Certification

The system self-assessment is only one component of the entire BMMP system review process required to obtain OUSD(C) certification. Reference the BMMP System Review Guidance for more information on the cost and business case analysis. Investment packages for systems and operational systems with a current year investment budget of greater than $1,000,000 are forwarded to BMSI for evaluation and to obtain the Comptroller's certification. Investment packages for systems of $1,000,000 or less are forwarded to the Deputy Chief Financial Officer for certification.